AMENDMENTS TO THE CLAIMS

CLAIMS (clean copy)

1. (currently amended) A distributed subscriber management method for controlling user authentication at an access control node located between a plurality of user networks and an access network, the access network being connected to an external network having an access rights authentication server, the method comprising the steps of:

(a) receiving, at the access control node, which is operatively connected to the plurality of user networks, a data unit from a user located on one of the plurality of user networks;

(b) determining whether the data unit requires authentication;

(c) if the data unit requires authentication, determining whether authentication data is locally stored on the access control node,

(d) if the authentication data is locally stored on the access control node, authenticating the data unit, thus preventing unnecessary traffic interchange between the access network and the plurality of user networks;

(e) if the authentication data is not locally stored on the access control node, determining whether the data unit is eligible for transmission to the external network; and

(f) if the data unit is eligible for transmission, transmitting said data unit from the access control node to the authentication server of the external network.

2. (currently amended) The distributed subscriber management method as claimed in claim 1, wherein the step (d) includes interrogating the user for access information.

3. (currently amended) The distributed subscriber management method as claimed in claim 1, wherein the step (f) comprises a step of receiving, at the access control node, an

authentication message for said data unit from the authentication server to permit the user to access the external network.

4. (currently amended) The distributed subscriber management method as claimed in claim 1, wherein the step (b) comprises a step of searching the authenticated data unit locally stored on the access control node.

5. (currently amended) The distributed subscriber management method as claimed in claim 2, further including encrypting the access information at the access control node prior to transmitting the access information to the authentication server of the external network.

6. (currently amended) The distributed subscriber management method as claimed in claim 3, wherein the step of receiving, at the access control node, the authentication message for said data unit comprises a step of storing authenticated data unit in a local authorization table on the access control node.

7. (currently amended) The distributed subscriber management method as claimed in claim 6, wherein the step (b) comprises searching the authenticated data units stored in the local authorization table on the access control node.

8. (currently amended) The distributed subscriber management method as claimed in claim 3, wherein the step (f) comprises a step of communicating with the authentication server employing one or more of standard authentication protocols selected from the list consisting of remote authentication dial-in user service protocol, password authentication protocol, challenge handshake authentication protocol, and terminal access controller access control system protocol.

9. (currently amended) The distributed subscriber management method as claimed in claim 1, wherein the step (d) comprises employing one or more of standard authentication protocols selected from the list consisting of remote authentication dial-in user service protocol,

password authentication protocol, challenge handshake authentication protocol, and terminal access controller access control system protocol at the access control node.

10. (currently amended) The distributed subscriber management method as claimed in claim 3, wherein the step (f) further includes packet-labeling of the data unit.

11. (currently amended) The distributed subscriber management method as claimed in claim 6, wherein the step of receiving the authentication message further includes determining the contents of the authentication message at the access control node.

12. (currently amended) The distributed subscriber management method as claimed in claim 1, wherein the step (e) comprises examining the content of the authenticated data unit at the access control node.

13. (canceled)

14. (original) The distributed subscriber management method as claimed in claim 1, further including collecting statistical usage information at the access node.

15. (currently amended) An integrated access device, for placement between a user network and an external network, the external network having an access rights authentication server, the integrated access device comprising:

a user network interface for operatively connecting to a plurality of user networks to receive data units from the plurality of user networks;

an authentication agent, operatively connected to the user network interface for locally authenticating, authorizing and forwarding data units received from the plurality of user networks;

an external network interface, operatively connected to the authentication agent, for forwarding data units locally authorized by the authentication agent to the external network; and

means for communicating with the access rights authentication server of the external network.

16. (original) An integrated access device as claimed in claim 15, wherein the user network interface includes a plurality of ingress cards and the external network interface includes an egress card.

17. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent includes a local authorization table for authorizing data units.

18. (original) An integrated access device as claimed in claim 15, wherein the authentication agent includes network address assignment and release means.

19. (currently amended) An integrated access device as claimed in claim 15, further including service level enforcing means, network resource management means, means for statistical usage collection, and alarm monitoring means.

19. (canceled)

20. (canceled)

20. (currently amended) An integrated access device as claimed in claim 17, wherein the means for communicating with the access rights authentication server comprises:

means for determining whether the data unit is eligible for transmission from the access control node to the authentication server of the external network;

means for transmitting the data unit from the access control node to the authentication server of the external network;

means for receiving, at the access control node, an authentication message for said data unit from the authentication server to permit the user to access the external network; and

means for storing authenticated data units in a local authorization table on the access control node.

21. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent includes a password authentication protocol.

22. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent includes a challenge handshake authentication protocol.

23. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent includes a terminal access controller access control system.

24. (currently amended) An integrated access device as claimed in claim 15, wherein the authentication agent includes a remote authentication dial-in user service protocol.

25. (new) An access control node, for placement between a plurality of user networks and an access network, the access network being connected to an external network having an access rights authentication server, the access control node comprises the integrated access device claimed in claim 15.